Solutions for exercises for TATA55, batch 4, 2021

January 11, 2022

1. (3p) Let $\alpha = \sqrt{2} + \sqrt[3]{5}$. Find the minimal polynomial of α over $\mathbb{Q}$ and the degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

   Solution: First, we note that $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ and that

   $$\begin{aligned}\alpha^0 &= 1\\ \alpha^1 &= \sqrt{2} + 5^{1/3}\\ \alpha^2 &= 2 + 2\sqrt{2} * 5^{1/3} + 5^{2/3}\\ \alpha^3 &= 2\sqrt{2} + 6 * 5^{1/3} + 3\sqrt{2}5^{2/3} + 5\end{aligned}$$

   These powers are linearly independent over $\mathbb{Q}$, so α is algebraic of degree 6, and $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

   We have that

   $$(\alpha - \sqrt{2})^3 = 5 = \alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2}$$

   so

   $$\alpha^3 + 6\alpha - 5 = 3\sqrt{2}\alpha^2 - 2\sqrt{2}$$

   hence

   $$(\alpha^3 + 6\alpha - 5)^2 = 2(3\alpha^2 - 2)^2$$

   The minimal polynomial is hence

   $$(t^3 + 6t - 5)^2 - 2(3t^2 - 2)^2 = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17,$$

   we do not need to check that this is irreducible!

2. (4p) Let F be a field with $q < \infty$ elements, and let K be an extension of F.

   (a) Prove that $a^q = a$ for all $a \in F$.

   (b) If $b \in K$ is algebraic over F, show that $b^{(q^m)} = b$ for some $m > 0$.

   Solution: If $a = 0$ then $a^q = 0$, if not, then $a^{q-1} = 1$ by Lagrange, hence $a^q = a$.

   Since b is algebraic, $F(b)$ is a finite field with q^m elements for some m. Apply the previous result.

3. (4p) Let $\alpha \in \mathbb{C}$. Then α is an algebraic integer iff it is the root of an equation of the form

$$\alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0, \qquad b_1, \ldots, b_m \in \mathbb{Z}$$

   (a) Show that an algebraic integer is algebraic over $\mathbb{Q}$.

   (b) Show that the converse does not hold.

   (c) Show that any element of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$ can be scaled by a positive integer to become an algebraic integer.

   (d) Show that $\sqrt{1/3} + \sqrt[3]{1/5}$ is not an algebraic integer; scale it with a positive integer so that it becomes one.

   Solution: The first part is obvious, and $\alpha = 1/2$ is a counterexample: if

$$(1/2^m) + b_1(1/2^{m-1}) + \cdots + b_m = 0, \qquad b_1, \ldots, b_m \in \mathbb{Z}$$

   then multiplying with 2^m we get

$$1 + 2b_1 + \cdots + 2^m b_m = 0, \qquad b_1, \ldots, b_m \in \mathbb{Z}$$

   yet the LHS is odd.

   Suppose that $\alpha \in \mathbb{Q}$ is algebraic, satisfying

$$\alpha^k + a_{k-1}\alpha^{k-1} + \ldots a_1\alpha + a_0 = 0, \qquad a_j \in \mathbb{Q}$$

   Note that there is no restriction in assuming that the defining relation is monic, since this is over $\mathbb{Q}$. Suppose that $a_j = b_j/c_j$, with $b_j, c_j \in \mathbb{Z}$, $\gcd(b_j, c_j) = 1$. Put $N = \operatorname{lcm}(c_1, \ldots, c_{k-1})$. Then, multiplying with N^k we get

$$(N\alpha)^k + a_{k-1}N(N\alpha)^{k-1} + \ldots a_1N^{k-1}(N\alpha) + N^k a_0 = 0,$$

   which shows that $N\alpha$ is a zero of the polynomial

$$t^k + a_{k-1}Nt^{k-1} + \ldots a_1N^{k-1}t + N^k a_0$$

   Finally, we calculate that $\sqrt{\frac{1}{2}} + \left(\frac{1}{5}\right)^{\frac{1}{3}}$ is a zero of the irreducible monic polynomial

$$x^6 - x^4 - \frac{2}{5}x^3 + \frac{1}{3}x^2 - \frac{2}{5}x + \frac{2}{675}$$

   so $675a$ is an algebraic integer.

4. (4p) Recall that a field isomorphism is a ring isomorphism preserving the multiplicative identity, and that a field automorphism is a field isomorphism from the field to itself.

   (a) Prove that complex conjugation is a field automorphism.

(b) What are the field automorphisms of $\mathbb{Q}$?

(c) What are the field automorphisms of $\mathbb{Q}(\sqrt[3]{2})$?

(d) What are the field automorphisms of a field with 27 elements?

Solution: : The first is straight-forward:

$$\begin{aligned}\overline{z+u} &= \bar{z}+\bar{u}\\ \overline{zu} &= \overline{z}\overline{u}\\ \bar{\bar{z}} &= z\end{aligned}$$

An automorphism ϕ of $\mathbb{Q}$ satisfies $\phi(1)=1$ and also $\phi(n)=n$ for $n\in\mathbb{Z}$, so

$$\phi(m/n)=\phi(m)\phi(n)^{-1}=mn^{-1}=m/n$$

and is thus the identity.

For the third part, first observe that an automorphism of $\mathbb{Q}(\sqrt{2})$ must fix $\mathbb{Q}$, and send a zero of

$$t^3-2=(t-\sqrt[3]{2})(t^2+2\sqrt[3]{2}+\sqrt[3]{4})$$

to another zero. The last two zeroes are complex, hence $\phi(\sqrt[3]{2})=\sqrt[3]{2}$. Hence ϕ fixes not only $\mathbb{Q}$ but the whole of $\mathbb{Q}(\sqrt{2})$, so it is the identity.

For the fourth part, we note that any automorphism of $\mathrm{GF}(3^3)$ must fix the prime subfield $\mathbb{Z}_3$. We know that the frobenius automorphism $\phi(x)=x^3$ is an automorphism of $\mathrm{GF}(3^3)$, as is of course all powers of it; but

$$\phi^3(x)=x^{27}=x$$

so

$$\phi^j=\phi^k \quad\Longleftrightarrow\quad j\equiv k \mod 3$$

We claim that any automorphism is in fact Id, ϕ, or ϕ^2. To see this, let σ be any automorphism and let β be a primitive element of $\mathrm{GF}(27)$, with minimal polynomial

$$f(x)=x^3+a_2x^2+a_1x+a_0\in\mathbb{Z}_3[x].$$

Then

$$\begin{aligned}0&=\sigma(\beta^3+a_2\beta^2+a_1\beta+a_0)\\ &=\sigma(\beta)^3+a_2\sigma(\beta)^2+a_1\sigma(\beta)+a_0\end{aligned}$$

so $\sigma(\beta)$ is a zero of $f(x)$. However, we claim that the zeroes of $f(x)$ are β,β^3,β^9. Assuming this, $\sigma(\beta)$ is either β, β^3, or β^9, and since β is a generator of the cyclic multiplicative group of $\mathrm{GF}(27)$, σ is either identity, cubing, or raising to ninth power.

We pove prove that β^3 is a zero of $f(x)$, the case for β^9 is similar. We have

$$\begin{aligned} f(\beta^3) &= \beta^9 + a_2\beta^6 + a_1\beta^3 + a_0 \\ &= \beta^9 + a_2^3\beta^6 + a_1^3\beta^3 + a_0^3 \\ &= (\beta^3 + a_2\beta^2 + a_1\beta + a_0)^3 \\ &= f(\beta)^3 \\ &= 0 \end{aligned}$$

5. (4p) Let $\alpha \in \mathbb{C}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$. Put $\beta = \alpha^3$.

   (a) What is $[\mathbb{Q}(\beta) : \mathbb{Q}]$?

   (b) If $\alpha^5 = \alpha - 1$, what is the minimal polynomial of β?

   Solution: Clearly $\beta \in \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$. We also have that $\beta \notin \mathbb{Q}$, so $[\mathbb{Q}(\beta) : \mathbb{Q}] \neq 1$. Since this number divides $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, it must be equal to 5, so $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

   Now assume that α has minimal polynomial $x^5 - x + 1$. Then

$$\begin{aligned} \beta^0 &= 1 \\ \beta^1 &= \alpha^3 \\ \beta^2 &= \alpha^6 = \alpha^2 - \alpha \end{aligned}$$

   and so on; by linear algebra, we find the relation

$$\beta^5 + 3\beta^2 - \beta + 1 = 0$$

6. (6p) Let $F = GF(9)$, expressed as $\mathbb{Z}_3[y]/(y^2 + 2y + 2) \simeq \mathbb{Z}_3(a)$.

   (a) There are of course 9 irreducible monic linear polynomials in $F[x]$; how many irreducible quadratic polynomials are there?

   (b) The following sequence of elements in F is periodic; enough of it is given that you will be able to deduce the period.

$$\begin{aligned} (c_j)_{j=0}^{\infty} = (&2*a+1, 1, 2, 2*a+2, 2, 2*a, 0, a+1, a+1, 2*a, 2, a, 2*a, \\ &a+2, 2*a, 2*a+2, 0, 2*a+1, 2*a+1, 2*a+2, 2*a, a+1, 2*a+2, 1, 2*a+2, a+2, \\ &0, 2, 2, a+2, 2*a+2, 2*a+1, a+2, a, a+2, 1, 0, 2*a, 2*a, \\ &1, a+2, 2, 1, a+1, 1, a, 0, 2*a+2, 2*a+2, a, 1, 2*a, a, 2*a+1, \\ &a, a+1, 0, a+2, a+2, a+1, a, 2*a+2, a+1, 2, a+1, 2*a+1, 0, 1, 1, 2*a+1, \\ &a+1, a+2, 2*a+1, 2*a, 2*a+1, 2, 0, a, a, 2, 2*a+1, 1, 2, 2*a+2, 2, 2*a, \\ &0, a+1, a+1, 2*a, 2, a, 2*a, a+2, 2*a, 2*a+2, 0, 2*a+1, 2*a+1, 2*a+2, 2*a, a+1, 2*a+2, \\ &1, 2*a+2, a+2, 0, 2, 2, a+2, 2*a+2, 2*a+1, a+2, a, a+2, 1, 0, 2*a, 2*a, 1, \dots) \end{aligned}$$

   Find this period (and preperiod, if applicable).

(c) Find the recurrence relation over F that this sequence satisfies.

(d) Find the generating function of the sequence.

(e) Factor the denominator of the generating function (over some explicit extension of F), then perform partial fraction decomposition of the generating function.

(f) Find an explicit formula for c_j of the form

$$c_j = u\alpha^j + v\beta^j$$

where u, v, α, β lies in some (explicit) extension of F.

Solution: The methods in the lecture notes work also for irreducible monic polynomials in $GF(9)$. The number of quadratic monic irreducible polynomials is

$$\frac{1}{2}\left(\mu(2)9^1 + \mu(1)9^2\right) = 36$$

and if we want all irreducible quadratic polynomials there are $8 * 36 = 288$ such.

Next, we deal with (b), (c), (d). The Maclaurin expansion of order 6 of the GF is

$$2a + 1 + x + 2x^2 + (2a + 2)\,x^3 + 2x^4 + 2ax^5 + O(x^6)$$

and the $(2-2)$ Padé approximant of that is computed by SAGEmath to be

$$\frac{f(x)}{g(x)} = \frac{x + a + 1}{x^2 + (2a + 1)\,x + a + 2}$$

We get the same rational function if we include the first 7, or 8, or 9, or 50, terms, so we are reasonable sure that we have found the correct GF.

Since the denominator is of degree 2, we expect a period length of $9^2 - 1 = 80$, and this holds true for the given initial segmment, with pre-period length zero.

Now for the remaining questions. The splitting field of $g(x)$ is

$$\frac{F[y]}{y^2 + (2a + 1)\,y + a + 2} \simeq GF(3)(b)$$

with $b^4 + 2b^3 + 2 = 0$. In the splitting field, we have that

$$a = 2b^3 + 2b^2 + 1$$

so we translate everything to this field:

$$\begin{aligned} f &= x + 2b^3 + 2b^2 + 2 \\ g &= x^2 + \left(b^3 + b^2\right)x + 2b^3 + 2b^2 = (x + 2b^2 + b + 1) \cdot (x + b^3 + 2b^2 + 2b + 2) \\ GF &= b^3 + b^2 + x + 2x^2 + \left(b^3 + b^2 + 1\right)x^3 + 2x^4 + \left(b^3 + b^2 + 2\right)x^5 + O(x^6) \end{aligned}$$

We denote the zeroes of g by

$$\sigma = b^2 + 2b + 2, \qquad \tau = 2b^3 + b^2 + b + 1$$

The partial fraction decomposition then is

$$\begin{aligned}
\frac{f(x)}{g(x)} &= \frac{2b^3 + 2b^2 + 2b + 2}{x + 2b^2 + b + 1} + \frac{b^3 + b^2 + b + 2}{x + b^3 + 2b^2 + 2b + 2} \\
&= \frac{A}{x - \sigma} + \frac{B}{x - \tau} \\
&= \frac{A}{-\sigma} \frac{1}{1 - x/\sigma} + \frac{B}{-\tau} \frac{1}{1 - x/\tau} \\
&= \frac{-A}{\sigma} \sum_{j=0}^{\infty} x^j/\sigma^j + \frac{-B}{\tau} \sum_{j=0}^{\infty} x^j/\tau^j \\
&= \sum_{j=0}^{\infty} \left(\frac{-A}{\sigma^{j+1}} + \frac{-B}{\tau^{j+1}} \right) x^j
\end{aligned}$$

We check that

$$\begin{aligned}
s2 &= \frac{-A}{\sigma^{2+1}} + \frac{-B}{\tau^{2+1}} = 2 \\
s3 &= \frac{-A}{\sigma^{3+1}} + \frac{-B}{\tau^{3+1}} = b^3 + b^2 + 1 = 2a + 2 \\
s4 &= \frac{-A}{\sigma^{4+1}} + \frac{-B}{\tau^{4+1}} = 2
\end{aligned}$$